Remarks

35 USC 112

In general, amendments to the claims as a whole were made in response to the Rejection under 35USC 112 for claims 1-8, 10-14, 16-21 and the specification, in order to expedite prosecution of this application.

In particular, Applicant considers that the specification as originally filed does support the terminology of printing data in the claims. In particular, Applicant notes the following support, *emphasis* added:

Paragraph [0002] clearly introduces the use of printers as network resources in connection with data traffic over a network. "Local area networks are widely used as a mechanism for making available computer resources, such as file servers, scanners, and *printers*, to a multitude of computer users. It is often desirable with such networks to restrict user access to the computer resources in order to *manage data traffic over the network* and to prevent unauthorized use of the resources. Typically, resource access is restricted by defining access control lists for each network resource. However, as the control lists can only be defined by the network administrator, it is often difficult to *manage data traffic at the resource level*.".

Paragraph [0003] clearly states access to printing resources. "Recently, the Internet Print Protocol ("IPP") has emerged as a mechanism to control access to *printing resources over the Internet*. However, IPP is replete with deficiencies.".

Paragraph [0019] clearly states that transmitted data can include data typically printed. "In addition, the invention is not limited to only facilitating transmission of *text data*, but instead may be used to transmit *image data*, audio data or multimedia data".

Paragraph [0022] clearly states "Typically, each network resource 104 comprises *a printing device*".

Paragraph [0023] clearly states that the network resource is associated with application data. "enterprise responsible for administering the *network resource 104*, is provided with a network address corresponding to the enterprise, and includes a queue for receiving *application data*".

Paragraph [0058] clearly states that the application data is suitable for processing (e.g. printing) by the network device (e.g. printer as noted above). "passes the *application data* received from the application software to the resource driver 402 for translation into a *format suitable for processing by the selected network resource 104*".

However, even in view of the above stated support for the terminology of "printing data" that would be clear to a person skilled in the art when reviewing Applicant's disclosure, Applicant has amended the term "printing data" to refer to the more generic term of "application data" that can optionally include more that just data for printing by a printer embodiment of the network device. This amendment has been done to further expedite the prosecution of this application. Further, Applicant has amended the independent claims to refer to a more generic network resource rather than the specific "printer". In addition to these amendments, Applicant has included language in the dependent claims to refer to the application data to include text data or image data which is consumable by a printer embodiment of the network resource.

Further support for other claim amendments can be found at least in the following places:

- Paragraph 64: "The polling server 116 then extracts the network address from the received application data, and transmits the application data to the appropriate server 118 or network resource 104 for processing."
- Paragraph 24: "the polling server 116 transmits the application to the enterprise server 118 for distribution to the appropriate network resource 104."

- Paragraph 25: "The network address field 302 identifies the network address of the network resource 104. ... However, in the case where the network resource 104 comprises a non-IPP-compliant device ... the network resource 104 is linked to the communications network 112 via a suitable server, and the network address field 302 for the network resource 104 identifies the Internet Protocol ("IP") address of the server."

- Paragraph 59: "...and then transmits the resulting data over the communications network 112 to the network resource 104 at the specified network address..."

Accordingly, Applicant considers the rejection of the specification and for claims 1-8, 10-14, 16-21 under 35USC 112 as overcome.

35 USC 101

Applicant notes the rejection of claims 1,2,6-8,10,11,18,20 under 35 USC 101 as non-statutory subject matter.

Applicant has amended claim 1 to refer to the proxy server having a queue (see paragraph [0024] for support. Applicant considers the positive recitation of a memory construct such as a queue in connection with the storing of data in the memory construct to provide for the claimed invention to fall within at least one of the four categories of invention.

Accordingly, Applicant considers the rejection of claims 1,2,6-8,10,11,18,20 under 35 USC 101 as overcome.

35 USC 103(a)

Applicant has reviewed the rejection of claims 1-8, 10-14 and 16-21 under 35 U.S.C. 103(a) in view of Grantges (6,324,684) in combination with Nelson (6,553,422). Applicant has reviewed the disclosures of Nelson and Grantges and does not agree with the Examiner's interpretation thereof, in view of Applicant's

pending claims 1-8, 10-14 and 16-21. Applicant has the following comments on Nelson and Grantges.

In general terms, Applicant is confused as to the continued rejection of the claimed polling and pulling from inside of a firewall of data stored outside of the firewall, by using prior art that only teaches synchronous transfer of data over networks. Applicant considers the cited references to date to be completely deficient for use in supporting Examiner arguments trying to show asynchronous data transfer in the cited art.

Further, Applicant notes that Nelson, Grantges , and Remer are also silent as to the claimed feature of "the polling server for inhibiting exposure to security breaches associated with firewall access ports". Accordingly, Applicant considers the teachings of the cited references to data as deficient in view of the novel and non-obvious invention as presently claimed.

Grantges

Applicant confirms the correctness of the Examiner's statement of "However, Grantges failed to teach a polling server located logically behind the firewall, the polling server being configured for polling the proxy server to pull the received printing data across the firewall from the queue of the proxy server to the polling server".

Indeed, Applicant agrees with the Examiner that one cannot find any mention or suggestion of polling in the disclosure of Grantges, since the act of polling implies an *asynchronous* transfer of data between the sender and the recipient of the data. Instead, Grantges is focused on *synchronous* transfer of data, which is contrary to Applicant's claimed invention. This is evidenced through the teachings of Grantges, namely paragraph 4 (given below with *emphasis* added) of the Detailed Description of the Preferred Embodiment, again in detail further in the text, and in the flow diagram of Figure 2, which shows initiation of the synchronous data communication process from *outside* (i.e. network side) of the firewall.

"Before proceeding to a detailed description of computer system 20, a general overview of the operation established by the invention will be set forth, as viewed by user 18 of client computer 22. Initially, user 18 of client computer 22 enters the destination URL into a web browser portion of client computer 22. The web browser then issues an HTTP request across insecure network 26, which is routed to proxy server 34. The user 18 may then be presented with a "popup" message that a secure network connection is about to be established. The message may also ask which X.509 digital certificate user 18 wishes to use for authentication. The user-selected X.509 digital certificate is then sent to proxy server 34. At this point, a first level authentication is conducted, outside the firewall, by proxy server 34 (e.g., checks to see whether the X.509 certificate has been issued by a predetermined preapproved certificate authority). *If authenticated at this level, proxy server 34 then sends the information contained in the client's digital certificate through firewall system 32 to gateway 38* to be authenticated at a second, more substantive level. The second level authentication involves examining the particulars of the X.509 digital certificate using the data stored on authorization server 46. If user 18 is authorized to access multiple applications, the next item after the "popup" message to be displayed to user 18 is an "options page", presenting the multiple choices. Once a particular application is selected, the next item to be displayed for user 18 is a welcome page of the selected application. Secure, authenticated remote access is complete. In accordance with the present invention, computer system 20 provides an efficient mechanism for routing the remote user 18 of client computer 22 to the selected application being served by one of the destination servers."

Accordingly, Applicant submits that the proper interpretation of Grantges is that the data communication process is initiated by the client computer 22, which sends a message to the proxy server 34, which then goes through the firewall, first to gateway 38. It is only after that, does the interaction with the proxy server

40 happen. So in Grantges, Applicant submits that the data communication process is *synchronous*, as it is initiated by the client 22 and requires a port to *already* be open inbound in the firewall, which is contrary to the claimed invention of "pull any said received printing data". Applicant emphasizes that the gateway server 38 of Grantges has to be contacted first from outside of the firewall, before the process of proxy server 40 (inside the firewall) commencing communication with proxy server 34 (outside the firewall).

In addition, Applicant has reviewed the disclosure of Grantges and cannot find the Applicant's claimed element of "the proxy server configured for storing the received application data in queue".

Accordingly, in view of the above discussion, Applicant submits that Grantges does not teach any reference to asynchronous communication of data through a firewall, nor does Grantges teach the use of a queue to facilitate that asynchronous communication. In fact, Grantges can only be attributed to the teachings of generic *synchronous* network communications that are *initiated from a remote location* (e.g. client 22) and directed to a local location (e.g. through proxy server 40).

Nelson

Applicant has reviewed the teachings of Nelson and cannot find any reference or suggestion of polling through a firewall, as suggested by the Examiner.

Applicant has found a direct reference to polling in Nelson in column 4 - line 65 to column 5 - line 8, however only in relation to an email server 135 that is not described as used in combination with the server/firewall 145 (see also Figure 2). Further, Applicant submits that, clearly, Figure 2 shows a direct connection (that bypasses the server/firewall 145) between the email server 135 and the remote processor 157, as well as a direct connection (that bypasses the server/firewall 145) between the local processor 122 and the email server 135. Accordingly, Applicant submits that email communications of Nelson are sent directly over the Internet 150 from the processor 157 to the email server 135, which is then

periodically polled (without interaction through the server/firewall 145) by the local processor 122.

In view of the above discussion and cited portions of Nelson, Applicant submits that asynchronous email communication (i.e. "periodically polls email server 135") was known by Nelson at least as of the filing date of the 6,553,422 patent, but not in relation to a firewall. Applicant argues that if Nelson intended their teachings to include polling initiated from inside of a firewall, they would have taught such explicitly. Instead, Nelson mentions firewall and the act of polling *but in separate contexts* that are clearly not related in any manner and are therefore disconnected. In other words, there is no motivation to be found in Nelson that would lead one of ordinary skill in the art to combine the teachings of polling and use of a firewall, except with direct knowledge of Applicant's teachings which is impermissible hindsight.

Applicant has also reviewed the teachings of Nelson as cited by the Examiner, as well as the Abstract. In response, Applicant cannot find any direct teachings in Nelson that provide for the architecture of a proxy server with a queue that is "located logically outside the firewall" and a polling server that is "located logically inside the firewall", as presently claimed. Instead Applicant submits that Nelson describes a fundamentally different network communications architecture of: a remote processor 157 (of machine 70); the Internet 65; a machine/firewall 60 and a local processor 122 (of machine 50). Applicant argues that only Nelson's machine 70 is external to the machine/firewall 60 (and does not function as "a proxy server" as proposed, rather as a provider of instructions based on *synchronous* communications implemented between the machines 70,50, which are on either side of the machine 60 that *acts* as a firewall. Accordingly, Applicant submits the Examiner cited combination (in Nelson) of a proxy server, a network, a firewall, and a polling server (in communication with the proxy server through the firewall over the network) is simply not provided in Nelson.

However, if the Examiner chooses to ignore the fact that the claimed combined features of a proxy server, a network, a firewall, and a polling server are not disclosed in Nelson, Applicant further submits that Nelson only teaches

synchronous communications between the machines 70,50, which is contrary to the Examiner's purported findings in Nelson of "polling the proxy server to pull the received printing data". Applicant notes that Nelson teaches the initiation of communication from inside of the machine/firewall 60 by the local processor 122 through sending of a message via the machine 60 over the Internet 65 to the remote processor 157, thereby prompting the remote processor 157 to send a command back to the local processor 157. However the difference between this message communication of Nelson and Applicant's claimed invention is that Nelson's communications (i.e. request 75,170 and corresponding response 76,171, see column 2 lines 30-37 and Figures 1,2) are *synchronous* in nature and do *not* involve any use of polling (as presently claimed) to provide for *asynchronous* communications. Explicit confirmation of this synchronous deficiency in Nelson can be found in column 6, lines 50-55 as "every message sent from the remote processor to the local processor *must be preceded* by an authorization from the local processor", *emphasis* added. This authorization from the local processor is included in the messages that are communicated from the local processor to the remote processor, via the machine 60.

Further, as provided by the teachings of Nelson, the remote machine does not involve a queue, as presently claimed, since the remote machine does not expect a request message from the local machine until the request message is received. Once the request message is received, then the remote machine formulates an appropriate response message (on a per request message basis – see column 2 lines 29-36) and sends back this formulated message to the local machine, hence the synchronous nature of the machine 50,70 communication.

In view of the above, Applicant argues that Nelson process when applied to Applicant's system in the current application would be for the local printing device 104 to send a request to the remote terminal 200 to begin sending a print job back to the printer. This synchronous communication process is not what is being claimed by the Applicant, rather the use of a queue at the proxy server, located outside of the firewall, to allow application data (e.g. print data) to be stored until a poll request is received through the firewall from the polling server.

The poll request seeks to determine if any application data is available in the queue, and if so then proceeds to pull the application data back through the firewall. This asynchronous transfer of the application data from the terminal to the network resource (e.g. printer) provides for an advantage not given in either Grantges or Nelson, namely the ability to open a port in the firewall at the choosing of the polling server, rather than leaving a port in the firewall open (a security risk) for receiving the application data unannounced from the network terminal. Applicant submits that neither Grantges nor Nelson explicitly teaches the use of polling through a firewall asynchronously, initiated from inside of the firewall, in order to obtain any available application data stored in a queue resident outside of the firewall.

Further, Applicant submits that the referenced teachings of Remer are also directed to synchronous communications and do not contemplate, implicitly nor explicitly, the use of polling from inside of a firewall as claimed. Applicant also notes that Nelson, Grantges , and Remer are also silent as to the claimed feature of "the polling server for inhibiting exposure to security breaches associated with firewall access ports". Accordingly, Applicant considers the teachings of the cited references to data as deficient in view of the novel and non-obvious invention as presently claimed.

Accordingly, Applicant considers the rejection of claims 1-8, 10-14 and 16-21 under 35 U.S.C. 103(a) as overcome.

Conclusion

In light of the above submissions and remarks, applicant submits that claims 1-21 are in condition for allowance, and request that the outstanding rejections be withdrawn. If a telephone conference would expedite allowance of the claims, the

Examiner may wish to telephone Applicant's Patent Agent at (416) 862-4318.

Respectfully submitted,

Gowling Lafleur Henderson LLP as agent for Grant Tisdall

Grant Tisdall
Registration No. 53,902

Gowling Lafleur Henderson LLP
Suite 1600, 1 First Canadian Place, 100 King Street West
Toronto, Ontario
Canada M5X 1G5
(416) 862-7525

TOR_LAW\ 7119795\3